FIDO2 / Web Authentication

Einde der wachtwoorden?

Joost van Dijk

9 april 2019 - What’s next @ SURFconext?


10:26
Saturday, May 12
KRYPTON
now
facebook.com
signed in

sa.test.surfconext.nl/registration/select-token

Registration Portal

Authentication in two steps

English

Sign out

1. Select token
2. Link token
3. Confirm
4. Activate token

Select token

SMS

Log in with a one time SMS code. For all mobile phones.

Select

Tiqr

Log in with a smartphone app. For all smartphones with Apple iOS or Android.

Select

YubiKey

Log in with a USB hardware token. For all devices with a USB port.

Select

U2F

Sign in with a U2F device.

Select

Voordelen

- W3C standaard API
- Driverless
- *Device attestation*
- Public Key crypto (ECC)
- Privacy friendly (elke site een eigen key)
- *Phishing protection*
- Passwordless
- Goedkoop: hardware €10-20

User verification

fido alliance

CTAP

USB/NFC/BLE

HTTPS

W3C®

WebAuthn API

Web Server

Challenge/Response authentication

Web Authentication

Phishing Protection

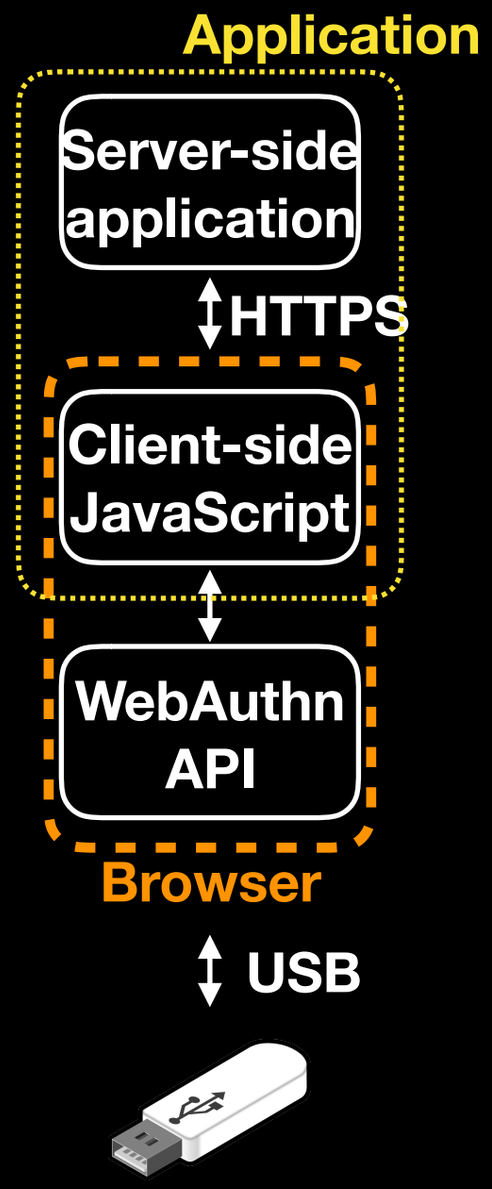
response = sign(k, challenge+origin)

result = verify(p, response)
and
check origin

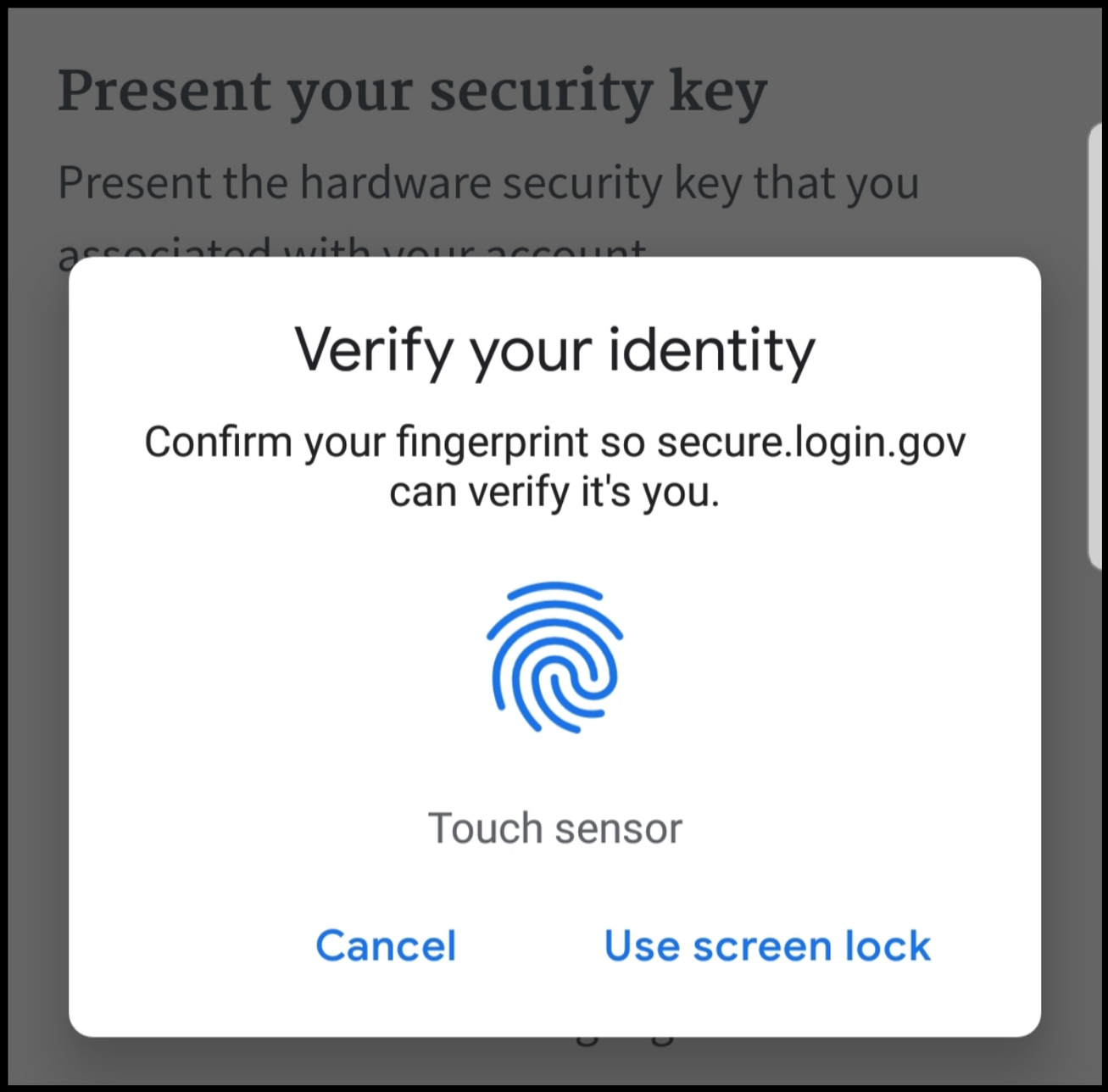
JavaScript API

- `navigator.credentials.create()`
  register new key

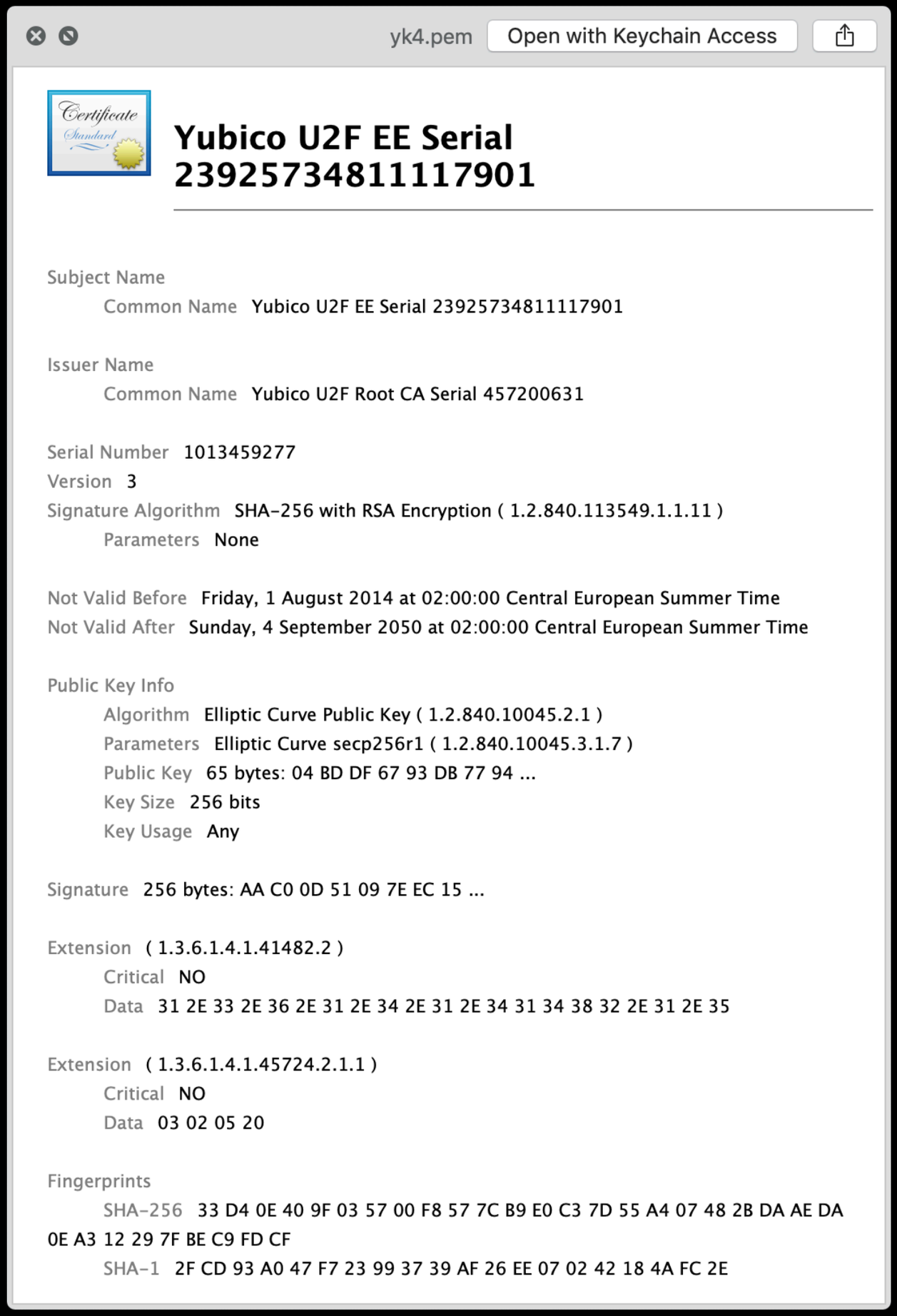
- `navigator.credentials.get()`
  authenticate using a
  previously registered key



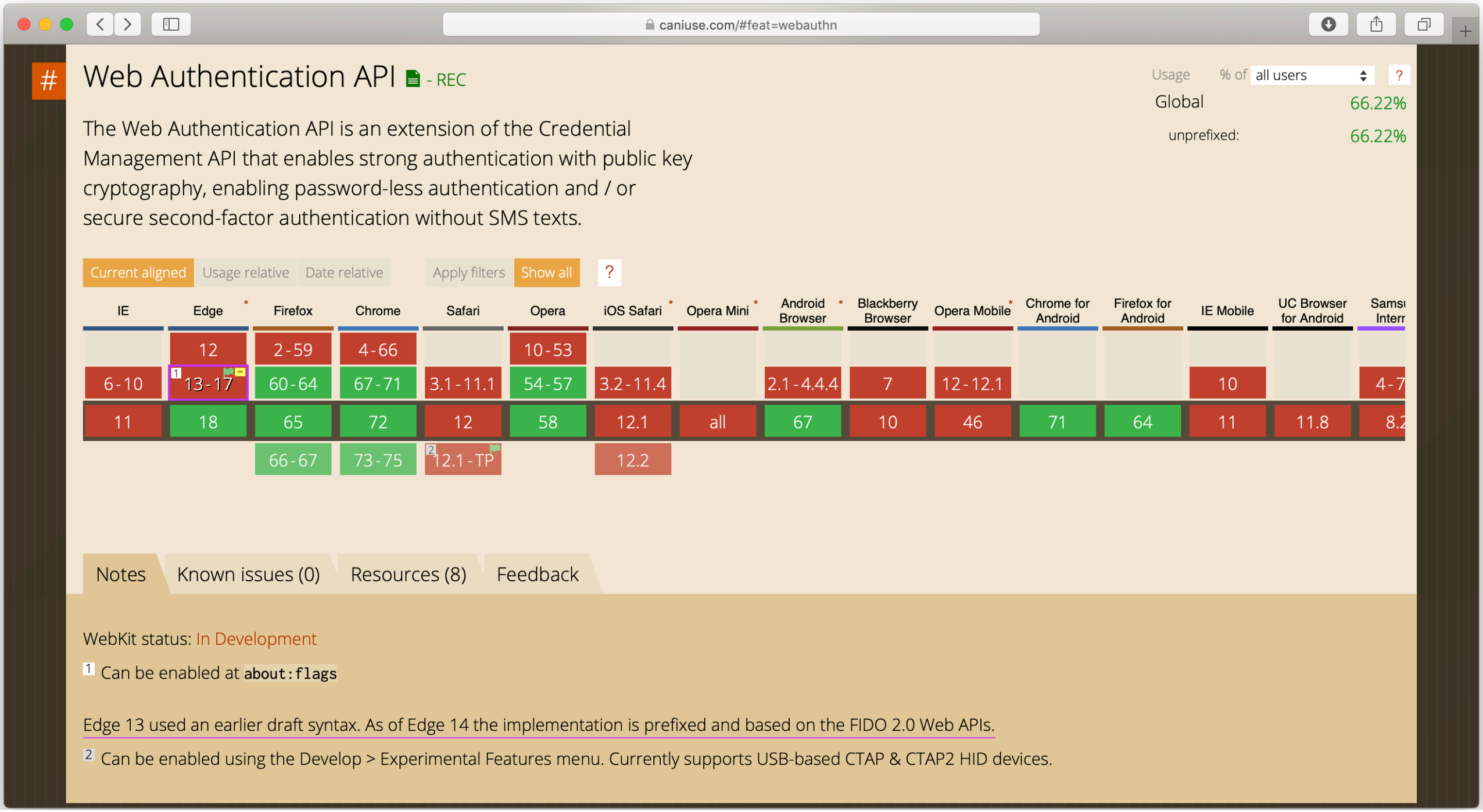
Platform Authenticator



Device Attestation



Browser Support



Questions?
Remarks?

Joost.vanDijk@surfnet.nl

http://nl.linkedin.com/in/joostd